1-1-2014

# E-Government users' privacy and security concerns and availability of laws in Dubai

Jawahitha Sarabdeen
*University of Wollongong in Dubai*, jawahith@uow.edu.au

Gwendolyn Rodrigues
*University of Wollongong in Dubai*, gwen@uow.edu.au

Sreejith Balasubramanian
*University of Wollongong in Dubai*, sbalasub@uow.edu.au

# Government Users' Privacy and Security Concerns and Availability of Laws in Dubai

**Jawahitha Sarabdeen**[1]
**Gwendolyn Rodrigues**[2]
**Sreejith Balasubramanian**[3]

**Abstract**

The purpose of the study was to review privacy and security concerns and their impact on e-Government adoption in Dubai. The research analyzed the literature on e-Government, security and privacy concerns of e-Government adoption and the legislative provision relating to privacy and security protection. A survey on e-Government user concern on privacy, security and ease of use was also carried out. The data for the survey in this research was collected from 190 respondents in Dubai. The results of the analysis revealed that perceived security, privacy and perceived ease of use were important constructs in e-Government adoption. The analysis of legal framework showed that the Federal Constitution, the Penal Code, the new Data Protection Act and the Computer Crime Act could be used to address various privacy and security concerns. Thus it is important that the policy makers facilitate an appropriate awareness campaign of the existence of both information privacy and security protection to attract more participation towards the e-Government services.

**Keywords: e-Government Adoption, Privacy, Security, Dubai Laws**

## Introduction:

The proliferation of e-Government services puts Dubai e-Governments ahead of a large number of those of other regional players. Research shows that there are various stages of e-Government development (Howard, M., 2001; Baum and Di Maio, 2000; Layne and Lee, 2001; Moon, M.J., 2002) and t-Government (Transactional Government) is the highest level of maturity for e-Government. At t-Government stage, government services are transparent and citizens are provided with a single contact point. Therefore, this phase brings with it a set of challenges

[1] Associate Professor, Faculty of Business, University of Wollongong in Dubai, P.O. Box: 20183, Dubai, United Arab Emirates, Tel: +971 4 3672455, Email: jawahithasarabdeen@uowdubai.ac.ae (Corresponding Author).

[2] Associate Professor, Faculty of Business, University of Wollongong in Dubai, P.O. Box: 20183, Dubai, United Arab Emirates, Tel: +971 4 3672431, Email:GwendolynRodrigues@uowdubai.ac.ae

[3] Institutional Research Officer, Office of Institutional Effectiveness, University of Wollongong in Dubai, P.O. Box: 20183, Dubai, United Arab Emirates, Tel:+971 4 367 2467, E-mail: sreejithsubramanian@uowdubai.ac.ae

(Layne and Lee, 2001). The transition from e-Government services to those of t-Government is important, however studies show that e-Government initiatives have stagnated at the transactional stage of development (Lee et. al., 2001; Sarikas and Weerakkody, 2007) due to the existence of various barriers.

The study looks at how far privacy and security act as barriers that caused e-Government users in Dubai to shy away from adopting fully functional e-government services. Dubai is specifically studied because the Dubai Government Strategy 2011-2013 "aims at developing an accountable and innovative government." The UAE, including Dubai, achieved 28$^{th}$ rank overall, according to the UN survey, as against 49$^{th}$ rank in the 2010 survey, and scored 7$^{th}$ rank on the online service index as against 99$^{th}$ rank in the 2010 Survey, and 6$^{th}$ rank on the eParticipation index and 86$^{th}$ rank in the 2010 survey. This study gives an insight to the relevance of legal developments in enhancing further the position of Dubai in e-government adoption. To the best knowledge of the researchers there was no substantial study conducted in Dubai on the impact of privacy and security on e-Government adoption; this study fills that gap.

In order to examine the privacy and security concerns of e-government users and the availability of laws in Dubai, the research paper is divided into 6 sections. Section 1 introduces the topic and the rationale for selecting Dubai for the study. Section 2 of the research explains the methodology employed. A dual methodology is adopted: (i) content analysis of the legal framework of Dubai regarding privacy and security; and (ii) a survey method to collect the opinions of e-government users. Section 3 reviews the important literature on privacy and security concerns in e-activities and e-government adoption. Section 4 undertakes an in-depth analysis of the opinion collected through stratified sample surveys. The surveys were collected from users of e-government services, which include expatriates and citizens, since the government is endeavoring to provide better legal framework and services for all e-government users regardless of whether they are expatriates or citizens. Section 5 covers the available laws and regulations in Dubai and the adequacy of laws in addressing privacy and security concerns in e-government adoption. Section 6 concludes with appropriate suggestions.

The research finding offers a substantial contribution to the government agencies that could require a distinction to be drawn between the adopters and non-adopters of e-government services and the reasons for non-adoption of those services. In addition, this paper also reports on residents' expectations and attitudes in relation to the privacy and security concerns. It also augments the awareness of the availability of legal provisions to protect privacy and security.

## 2. Research Methodology

The research looks at concerns about privacy and security of e-Government users. In order to analyse the concerns, a comprehensive analysis of a literature review was undertaken. The researchers also analyzed the legal framework of Dubai in addressing the privacy and security issues that might arise in adopting e-Government services. For this purpose the researchers used content analysis, as this methodology is generally helpful to analyse and explain the rules and principles relating to privacy and security laws. The research analyzed relevant legislation in

Dubai, which could possibly address the concerns. The case law was not included as in Dubai it is neither published nor available for the public.

The researchers also conducted a survey to collect the primary data of the residents of Dubai to understand their concerns. The objective of the survey was to explore the importance of privacy and security concerns and how these concerns might affect the customers' willingness to adopt e-Government services. For this survey a questionnaire was developed by the researchers and administered through field investigators. A paper-based survey was used over a period of 4 weeks, the focus being on university campuses and leading malls in Dubai. The purpose of choosing university campuses was to get the responses of the new generation, whom researchers believe are more Internet-oriented than is the previous generation. The purpose of selecting the leading malls in Dubai was to capture a stratified sample covering different nationalities and the local population. The complete survey examined more than 225 samples, however incomplete surveys and responses were removed, and a final set of 190 samples from varying ethnic and educational backgrounds was used for the analysis. As Dubai is a multicultural nation, with more than 80% of the population constituting expatriates, the authors believe the data collected provide an unbiased result grid that may be mapped by a follow-up study in other countries to tally the findings. Table A.1 shows the demography of the respondents to the survey. Coincidentally, the sample represented 20% of UAE nationals and 80% expatriate residents, which the researchers believe accurately represents the cultural composition of Dubai. The survey sought the attitudes of respondents on questions related to usability, navigation, privacy, security and reliability. Respondents were asked to rate each of the criteria on a 5-point scale.

| **Measure** | **Item** | **Frequency** |
|---|---|---|
| **Gender** | Male | 89 |
| | Female | 101 |
| **Nationality** | Expats | 152 |
| | UAE Nationals | 38 |
| **Education** | Masters | 54 |
| | Bachelors | 89 |
| | High schools or diploma | 47 |
| **Internet Usage** | High | 44 |
| | Moderately high | 55 |
| | High | 57 |
| | Moderately low | 22 |
| | Low | 12 |

Table A.1: Demographic profile of respondents

Since the researchers are investigating the attitudes of the respondents, they used the Likert Scale in analyzing their survey. Likert Scales have the advantage of not expecting a simple yes or no answer from the respondent, but rather allow for degrees of opinion. Therefore quantitative data obtained can be analyzed with relative ease. A Likert Scale assumes that the strength/intensity of experience is linear, i.e. on a continuum from strongly agree to strongly disagree, and makes the assumption that attitudes can be measured.

In order to analyze the results of the survey, factor analysis was performed. Factor analysis is a statistical method used to study the dimensionality of a set of variables. In factor analysis, latent variables represent unobserved constructs and are referred to as factors or dimensions. It is used to explore the dimensionality of a measurement instrument by finding the smallest number of interpretable factors needed to explain the correlations among a set of variables. Accordingly, the researchers performed factor analysis on the variable factors and identified the constructs. The constructs are named according to the grouping of variables based on past research. Constructs like perceived ease of use, perceived security and privacy were derived from various researches into privacy and security issues. Each variable is rated from strongly agree to strongly disagree.

The researchers conducted a Kaiser-Meyer-Olkin (KMO) measure of sampling adequacy and a Bartlett's Test to assess whether the patterns of correlations in the data indicated that a factor analysis was suitable. The ideal value of KMO is 1, and a Bartlett's Test should be significant ($p<.01$). The results obtained were that KMO = 0.801 showing the degree of common variance among the 6 variables was "fairly high" and the Bartlett's test was highly significant with $p<.005$, therefore factor analysis was suitable for this data set and the factors extracted accounted for a fairly high degree of variance. The rotated component matrix seen in Table B.2 shows how much each manifest variable loaded into each of the 2 latent variables. From this matrix it is easy to see that variables are loaded heavily into the construct 1 (one) and 2 (two).

| S.No | Variable | Construct 1 | Construct 2 |
|---|---|---|---|
| 1 | Usability | | 0.77 |
| 2 | Navigation | | 0.74 |
| 3 | Privacy | 0.88 | |
| 4 | Security | 0.83 | |
| 5 | Reliability | 0.79 | |

Table B.2: Rotated Component Matrix (Extraction Method: Principal Component Analysis, Rotation Method: Promax with Kaiser Normalization Rotation converged in 9 iterations)

The constructs are named according to the loaded variables in the rotated component matrix. Table C.3 gives the constructs and the grouped variables. The constructs are named according to the loaded variables in the rotated component matrix. Table C.3 also provides insights into each variable. Construct 1 is named Perceived Security and Privacy (PSP) while the Construct 2 is named Perceived Ease of Use (PEU) based on the variable loading into each construct. Overall satisfaction is our dependent variable and the two constructs act as the independent variables.

| Constructs | Criteria |
|---|---|
| **Perceived Security and Privacy (PSP)** | Privacy (Do you feel confident about your privacy while using e-government services?) |
| | Security (Do you consider your transaction is secure while using the e-government services?) |
| | Reliability (Do you consider that the e-government services provided are reliable?) |
| **Perceived Ease of Use (PEU)** | Usability (How do you perceive the ease of use of an e-government service?) |
| | Navigation (How easily do you consider you can navigate around an e-government website?) |
| **Overall satisfaction (OS)** | Are you satisfied with using e-government services? |

Table C.3: Variables & Constructs

Researchers used reliability analysis to ensure that the results were reliable. Reliability refers to the accuracy and precision of a measurement procedure. Reliability may be viewed as an instrument's relative lack of error. In addition, reliability is a function of properties of the underlying construct being measured, the test itself, the groups being assessed, the testing environment and the purpose of assessment. Reliability answers the question: How well does the instrument measure what it purports to measure? Some degree of inconsistency is present in all measurement procedures. The variability in a set of item scores is due to the actual variation across individuals in the phenomenon that the scale measures, made up of true score and error. Therefore, each observation of a measurement (X) is equal to true score (T) plus measurement error (e), or X = T + e. Another aspect of total variation is that it has two components: "signal" (i.e., true differences in the latent construct) and "noise" (i.e., differences caused by everything other than true differences). One type of diagnostic measure that is widely used and has been used in this study is the Cronbach's Alpha. The lower limit generally agreed upon for Cronbach's Alpha is 0.70. Cronbach's Alpha will generally increase as the inter-correlations among test items increase, and is thus known as "Internal consistency." Internal consistency estimates reliability of test scores. Inter-correlations among test items are maximized when all items measure the same construct. Since a reliability test was performed on each of the constructs separately, the results validated the model and factor analysis. The high alpha value of the constructs shows the variables within the constructs are correlated and 'measure the same thing'. The results of the reliability analysis are presented in Table D.4 and show that all of the constructs included in the study are strongly acceptable and have reliable coefficients. Hence, the results demonstrate that the questionnaire is a reliable instrument.

| Construct (number of items) | Cronbach's Alpha |
|---|---|
| Perceived Security and Privacy (3) | 0.7332 |
| Perceived Ease of Use (2) | 0.7238 |

Table D. 4: Reliability Analysis

Research model was developed to identify the significance and contribution of each construct to the overall satisfaction of e-Government services, which in turn reflects the e-Government Adoption. However the frequency of Internet usage was also considered since it is an important factor which contributes to e-Government adoption. The model developed is shown in figure A.1 and various hypotheses were formulated to test the model.

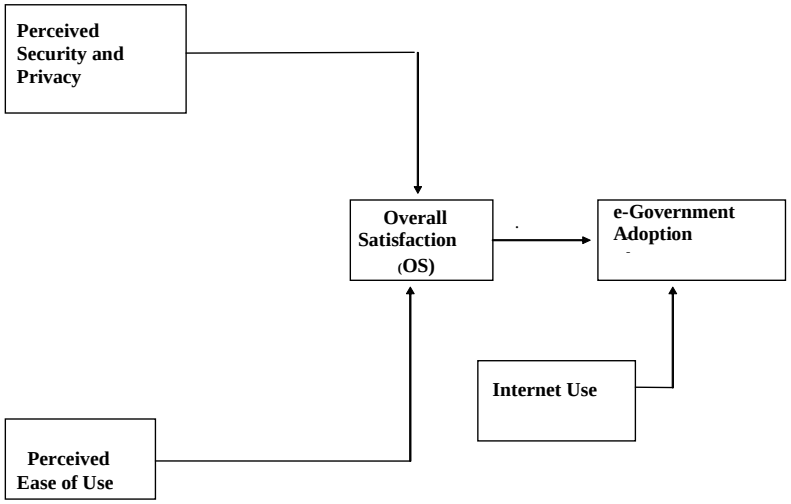


Figure A.1: The research model developed by researchers

The hypothesis derived from the model is H1, H2, H3 and H4. The hypotheses (H1 to H4) explain a cause-and-effect relationship of the various questions relating to e-Government adoption and how each construct contributes to overall satisfaction. The following hypotheses are:

H1: Perceived Security and Privacy (PSP) has a significant effect on overall satisfaction
H2: Perceived Ease of Use (PEU) has a significant effect on overall satisfaction
H3: Overall satisfaction (OS) has a significant effect on e-Government adoption
H4: Internet usage (IU) has a significant effect on e-Government adoption

Having understood the factors that lead to e-government adoption, it is also important to understand whether the incidence of e-government adoption differs from a demographic perspective. The hypothesis H5, H6 and H7 identify the demographic differences in e-Government adoption. The demographic profiles considered for the study are gender, UAE nationals and expatriates, and education levels of the respondents. The following hypotheses were derived to test any statistical differences existing amidst the demographics.

H5: E-Government adoption level is the same for male and female users
H6: E-Government adoption level is the same for expatriates and UAE nationals
H7: E-Government adoption level is the same irrespective of educational levels

Primary data from the research were analyzed to test the hypotheses and to determine whether any culling was necessary.

The main research limitation is that the questionnaire is not completely free of bias and was taken on a single occasion. User reactions change, and may depend on the environment. This study is limited only to users of e-government services and perceptions of non-users in regard to e-government services are not collected.

## 3. Literature Review

### 3.1. Privacy and Security Concerns of E-Activities:

Privacy violation concerns are increasing among Internet users due to proliferation of databases, collection of personal data and loss of control over the collected data (Culnan, 1993; Hiller and Cohen, 2001). The electronic frontier introduces new challenges to maintaining data privacy. Since 2005 more than 158 million data records of US residents have been exposed (Scheier, 2007). In 2007, more than 2.5 million credit card numbers were stolen online in a 12-month period (Scheier, 2007). A recent Gartner survey of 7,000 consumers showed that more than 80% were concerned about their social security and credit card numbers; 60% of those who participated agreed that security and privacy worries kept them away from online transactions (2011). Considering the inherent risks of transmitting sensitive information electronically, many citizens insist on assurances that their personal information will be kept confidential and that there will be no misuse of data. Opera Software's research in 2011 found that 25% of American respondents worried about privacy violations on the Internet whereas only 23% of Americans were concerned about declaring bankruptcy and 22% were afraid of losing their jobs. An additional 35% of respondents said they worry about the government's spying capabilities. Although nearly 80% of Americans reported that they have installed anti-virus solutions onto their computers in an effort to protect their privacy, only 61% said they use safe passwords (Personal Liberty News Desk, 2011). The surveys show that a customer's information is being viewed as a company's property, is a potential source of power and provides a competitive advantage. Thus there lies the likely tension between the businesses or government entities and users, as businesses and government continually strive to retain and utilize personal information of Internet users for mutual benefits. Owing to escalating concerns about national security,

governments are backing away from tougher privacy rules (Safire, 2002). These initiatives also aggravated the concern further.

The research on privacy and security violation started in the 1890s. However, from the 1960s (Westin, 1967), the research on corporate and public policy issues related to information privacy started to surface. From a business perspective, researchers analyzed risks associated with privacy violations (Bloom et al., 1994; Cespedes and Smith, 1993). Researchers also concentrated on governmental responses to privacy concerns (Clarke, 1999; Pincus and Johns, 1997; Reidenberg, 1996, Smith et al., 1996). Sheehan and Hoy (2000) measured the consumer online privacy concerns and Moon and Phelps researched the specific conditions under which consumers were willing to provide information (Moon, 2000; Phelps et al., 2000). The "power-responsibility equilibrium model" developed by Davis et al. (1989), states that power and responsibility should be in equilibrium; the business and government entities should have responsibility to ensure trust and confidence (Laczniak and Murphy, 1993). When the internet users perceive that businesses or governments act responsibly in terms of their privacy protection, assuring the existence of legal regulation to protect their privacy, trust and confidence will drive them to use the e-Government services.

Security and reliability concerns were identified as very important factors influencing consumer risk perceptions (Miyazaki and Fernandez, 2001; Suh and Han, 2003; and Wolfinbarger and Gilly, 2003). On the issue of security, consumer evaluations of an online retailer's security effectiveness (Lee and Turban, 2001) and perceived security control (Koufaris and Hampton-Sosa, 2004), consumers believed that the e-service provision of accurate and reliable services (Pitt et al., 1995) would contribute to the adoption of e-services. Culnan and Armstrong (1999) state that users conduct cost-benefit analyses when deciding whether to disclose confidential information. Strader and Shaw (1997) argue that consumers will not participate in e-activities if they feel the risk level, when compared with the benefit, is high. A survey conducted by Hoffman et al. (1999) showed a similar trend. According to the researchers, consumers' most cited reasons for rejecting online transactions were over their concerns about the lack of information privacy and the potential loss of control over confidential information. This finding supports the contention of Davis (1989), who stated that one of the factors that determined consumer adoption of technology was usefulness and ease of use (Davis, 1989). Perceived ease of use (PEOU) is the degree to which an individual believes that using a particular technology would be free of cognitive effort (Davis, 1989). It is shown that ease of understanding or use of a web site increases consumer trust in an e-commerce vendor. Thus it could build trust and could lead in reducing the perceived risk level (Pavlou, 2003). The Privacy-Trust-Behavioral-Intention model shows that there is a relationship between privacy concerns and willingness to provide personal information. Aprivacy protection policy in a website leads to trust and willingness to provide personal information. The research also showed that culture has a significantly moderating effect on the attitude of online users (Wu, Huang, Yen & Popova, 2012).

The research findings so far established that the concern for privacy and security protection is high, and the users who are concerned about privacy and security are cautious in providing personal or financial information; they expect the businesses and governments to take measures to ensure privacy and security of private data. The researchers also highlighted that the users are willing to participate in e-activities when they trust a particular business.

### 3.2 Theoretical Analysis of Privacy and Security Concerns of E-Government

Studies also have examined concern for privacy in relation to e-Government services (Dinev and Hart, 2006). The research focused on seven factors of privacy issues: perceived internet privacy risk, collection, error, secondary use, improper access, reputation and third party certificate. The perceived Internet privacy risk is the uncertainty associated with electronic transactions that are related to the loss of data due to an agency behaving opportunistically (Dinev and Hart, 2006; Kim et al., 2008). Collection of personal data refers to the personal information acquired by businesses or government agencies to complete electronic transactions (Smith et al., 1996; van Slyke et al., 2006). The major concern is that users doubt the ability of the collecting agency to obtain and store sensitive information securely. The privacy concern over potential error addresses the possibility of providing protection from accidental or intentional errors (van Slyke et al., 2006). Many citizens think that governments are not investing enough to safeguard their personal information. Unauthorized secondary use focuses on whether data collected for one purpose could be used for purposes other than the original purpose (van Slyke et al., 2006). Smith et al. (1996) investigated the concern over improper use of data internally and externally. According to Smith et al. (1996) and Solove (2006) improper access occurs when information is available to people not authorized to access that information. The likelihood of internal misuse of data is greater in the absence of an adequate guide on data access and use.

The reputation of a web site is a key factor in decreasing risk, developing trust (Kim et al., 2008) and building confidence among users of e-services. Citizens tend to trust organizations more if they have an established reputation. Reputation looks at overall perception of an entity based on one's experience with, knowledge of, and beliefs about the particular agency (Nam et al., 2006). This supports the earlier research that ease of use and ease of understanding a web site increases consumer trust, leads to reduction of the perceived risk level (Pavlou, 2003) and increases adoption of e-Government services.

Zhao & Zhao (2010) assessed the security of the U.S. state e-government sites to identify opportunities for and threats to the sites and their users. By using web content analysis, information security auditing, and computer network security, they found that most state e-government sites posted privacy and security policy statements; however, fewer than half stated clearly what security measures were in action. The major threats come from detectable main IP addresses and their ports (Bellamy et al., 2003). Lack of security created an anxiety among the users about e-government policy and the law relating to data sharing (Bellamy et al., 2005; Raab, 1998).

Bannister (2005) researched increasing vulnerability of citizens to breaches of privacy due to various government activities. He suggested mechanisms for striking a balance between ensuring security and the right to privacy. Foley et al. (2006) reviewed the activities, barriers, and future directions of information sharing for social inclusion in England, while Lam (2005) discussed the concept of collaboration in the information age by government agencies. Cullen (2009) analyzed the cultural relevance to the security and privacy concerns in the age of digital government. If the e-Government service is to be hosted using cloud computing facilities, a critical challenge is to

create consumers' trust by ensuring adequate privacy and security for consumer data. It is true that the computing and storage facilities are in the clouds and it is possible to use simple devices like cell phones to access them from anywhere in the world. But the convenience and ease of use should not be compromised with inadequate privacy and security protection. As the clouds are on the Internet, possible attack or intrusion might occur. In addition, the Cloud service providers have full access to consumer data, thus it is necessary for governments to take extra care about the protection and safety of personal data (Cheng & Lai, 2012). Another great challenge is regulating data kept in clouds beyond national borders and the geographical restriction of privacy protection laws. All the existing laws and regulations have restrictions covering data kept beyond national boundaries. Due to the inability of national laws and regulatory institutions to regulate data kept outside a particular country, the European Union's most important Directive for the protection of individual privacy, Directive 95/46/EC, imposes restrictions in term of coverage and trans-border data flow. In many countries there is no comprehensive regulation to govern data privacy and security within and beyond national borders. For example, in the USA, there is no federal legislation on privacy applicable to all states. The current legislative framework comprises federal and state privacy regulations for different industries. Thus there is no general provision on fair information practices for consumers' data (King & Raja, 2012). For instance, the USA's Privacy Act of 1974 regulated the government's use of personal information. It applies to all agencies working with personal information contained in a system of records. The e-Government Act required the government agents to conduct Privacy Impact Assessments in order to evaluate the impact of information technology on information privacy. The Health Insurance Portability and Accountability Act 1996 and American Recovery and Reinvestment Act 2009 regulate the government entities like the Health Insurance Company, health care clearinghouse and prescription Drug Card Sponsor (Khan, 2010).

The researches on the e-Government also show concerns about the possibility of privacy and security breaches. The users are afraid of "big-brother's" scrutiny of the users' private life due to disclosure of detailed private information. In addition, as most of the time, sensitive information is provided to successfully complete various integrated services of e-Government, the expectation of appropriate protection measure is high among users.

## 4. Survey Analysis of Privacy and Security Concerns of E-Government in Dubai

The research conducted in Dubai indicates that the users of e-Government are concerned about privacy and security. The researchers used a regression analysis to estimate the linear relationship between the dependent variable and the independent variables using the Statistical Package for the Social Sciences (SPSS). Multiple Linear Regression is used to investigate whether the variables in the constructs predict the overall satisfaction, and also to see which variables have the highest effect. The independent variables in the study were perceived as security and privacy (PSP) and perceived ease of use (PEU). The dependent variable in the study was overall satisfaction (OS).

The summary of the regression is given in Table E.5

| Model | R | R Square | Adjusted R Square | Std Error of the Estimate |
|---|---|---|---|---|
| 1 | 0.736 | 0.413 | 0.401 | 0.3564 |

Table E.5: Multiple Regressions: Model Summary
Predictors: (Constant), usability, navigation, privacy, security and reliability
Dependent Variable: Overall Satisfaction

The results show the following:

1. The 'r' value is 0.736, which means that all the chosen independent variables combined had a significant effect on the dependent variable: overall satisfaction. The multiple linear regressions performed to test the dependence of overall satisfaction on individual constructs measured separately showed that there was a significant relationship between overall satisfaction and all the constructs.
2. Perceived security and privacy had a significant effect on overall satisfaction and it was the most important construct. Perceived Comfort also had a direct link to overall satisfaction. The results of the analysis showed that those hypotheses H1, H2 were significant.
3. In order to determine if a relationship existed between the overall satisfaction, Internet usage and e-Government adoption, and the study ran a correlation between the two factors. The Table F.6 below shows the results of Pearson's correlation. There is a strong correlation (r>>.5) between OS and e-Government adoption.

| **Correlation** | **E-Government Adoption** |
|---|---|
| Overall satisfaction | r= .888** |
| Internet usage | r= .557* |

Table F.6: Correlation
**Correlation is significant at the 0.01 level (2-tailed),
* Correlation is significant at the 0.05 level (2-tailed)

**Comment [BDF1]:** Why Italic?

Similarly a Pearson's Correlation was run to examine the relationship between the time spent on the Internet and the e-Government adoption by consumers. There is a medium correlation (r>.5) between Internet usage and e-Government adoption. The results are statistically significant at 95% confidence interval. This is based on the assumption that frequent Internet users are much more likely to accept e-Government, and the correlation supports the hypothesis. The results show that the hypotheses H3 & H4 are significant. Figure B.2 summarizes the results with respect to the research model.

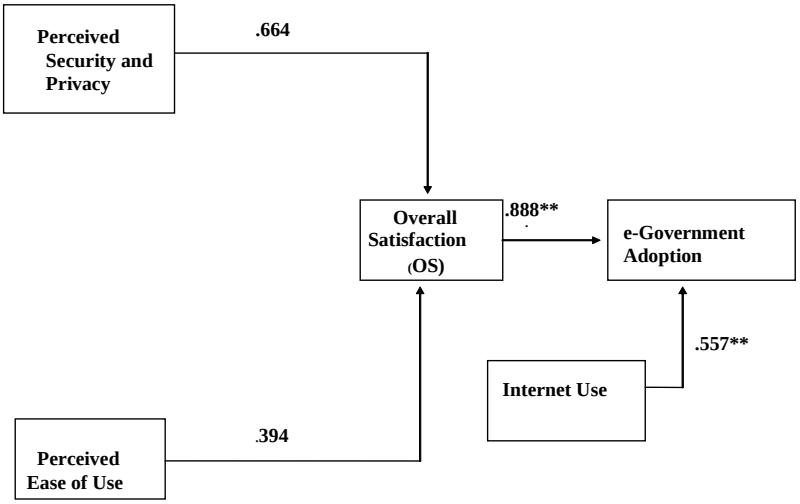


Figure B.2: Results of the multiple regressions on the model

4. The results of hypothesis H5 show that there is a significant difference in the e-Government adoption for male and female users. Female users are more reluctant than male users in e-Government adoption. However, hypotheses H6 and H7 could not identify any significant difference in e-Government adoption between expatriates and UAE nationals, and also between different educational levels.

| Hypothesis | Variable | Coefficient | Significance | Supported | Test performed | Contribution |
|---|---|---|---|---|---|---|
| HI | PSP & OS | 0.664 | 0 | Yes | Regression | High |
| H2 | PEU & OS | 0.384 | 0 | Yes | Regression | Moderately low |
| H3 | OS & E-Adopt | 0.888 | 0 | Yes | Correlation | Very high |
| H4 | IU & E-Adopt | 0.557 | 0.042 | Yes | Correlation | Moderately high |
| H5 | Gender & E-Adopt | 2.585 | 0.011 | No | t-test | Significant difference |
| H6 | Nationality & E-Adopt | 1.336 | 0.139 | Yes | ANOVA | No difference |
| H7 | Education & E-Adopt | 1.121 | 0.065 | Yes | ANOVA | Moderate difference |

Table G.7: Summary of results

The Table G.7 summarizes the overall study with the hypothesis test results. The finding of the survey reiterates the literature findings and show that Dubai residents, like residents in other countries are concerned about their privacy and the security of their personal data privacy. They also want to have reliable and facile websites and applications to facilitate adoption of e-

Government services. It also shows the direct relationship between the privacy and security concerns and intention to use the e-Government services. Even if the research shows that all participants, irrespective of their educational levels, are concerned about privacy and security, the female users are more so than the males. As Dubai e-Government users are concerned about privacy and security, the following section of the paper analyzes the available laws and regulations that could possibly be used to protect their privacy and security in case of abuse or misuse.

## 5. Dubai Legal Framework for Protection of Privacy and Security of e-Government Users

The Federal Constitution, the Penal Code and the new Data Protection Act and the Computer Crime Act could be used to protect various privacy and security concerns. The Federal Constitution in Article 31 clearly mentions that secrecy of communication and the information of the individual shall be protected. The provision could easily be applied to any kind of information or data. Thus, disclosure and usage of private information may be considered as a violation of the constitutional provisions. Additionally, the Penal Code in section 378 states that disclosure or use of any information or picture or view of a person's private life is a crime. Similarly section 379 states that any information received in confidence cannot be disclosed without the consent of the person who imparted in confidence.

The combined effect of these provisions is that any information or data received needs to be kept in private and it cannot be used or disclosed in any way without the consent of the data subject. The legal principles in these provisions are general and broad enough to cover privacy issues in e-Government service delivery. Thus collection, use, selling and distribution of any personal or private data could easily violate the right to privacy.

Dubai, the commercial state of UAE, has two other laws to regulate data privacy. They are Dubai Electronic Transactions and Commerce Law (No.2 of 2006) and Data Protection Law (DIFC Law No.1 of 2007). The Electronic Transaction and Commerce Law was passed to protect the interest of parties in electronic transactions. It also intended to define obligations, and enhance the application and reliability of e-commerce through legislative measures. Though there is no specific legislation to regulate e-Government activities, the e-commerce law can be extended to cover e-Government related activities and protection of data privacy and security of e-Government users. Article 27 specifically mentions the use of electronic records and signatures. Sub-section 1 of article 27 states that government departments can accept filing, submission, creation or retention of electronic records. The government also can issue any permit or license decision or approval in electronic format. The issue of privacy and security is very clearly addressed in article 31 of the e-commerce law. It states that any authorized person entrusted with personal information, who intentionally discloses the data in files, documents or communication, can face criminal charges. Unintentional or negligent disclosure on the part of authorized officials is also considered a criminal action.

However, this legislation has certain limitations. It excludes its application to "title deeds of immovable properties" and "negotiable instruments" including securities. Thus transfer, sale,

purchase of title deeds or negotiable instruments cannot be completed through e-Government facilities as the subject matter of such transactions is excluded from the ambit of the e-commerce law. This exclusion hinders the use of e-Government application of three major industries in Dubai: real estate, the financial sector and logistics. Fortunately, the e-commerce law article 2 allows the Council of Ministers to amend the exclusion clause. Thus it is hoped that the exclusions as to deed of immovable properties and negotiable instruments will be removed soon so many will be able to utilize the e-Government services for wider purposes.

The Data Protection Law (DIFC Law No.1 of 2007) follows the EU Data Protection Directive (95/46/EC) on personal data protection. The provisions are similar to the 1995 EU directive which introduced the "opt-in" system, in which obtaining consent of the users as stated in Article 8 is an important prerequisite to collect, store and use the personal data of data subject. The "data" could include any information relating to an identifiable person. Identifiable person is the one whose separate identity is ascertainable but who is not known in person. However, he can be traceable by various available factors. Personal data also includes any expression of opinion about the individual and any indication of the intentions of the data user in respect of that individual.

Article 8 also illustrates the mandatory principles when collecting, holding, processing or using personal data. The principles in Article 8 require

1. personal data to be processed fairly and lawfully. The data user must be informed of when and what personal data is collected and for what purpose they will be used. According to this principle the use of personal data for direct marketing purposes should also be prohibited. The provision outlaws direct marketing activities, the profiling of user data and use of those data for mass mailing purposes;
2. personal data to be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes. The use of excessive data is not allowed even though the data can be useful for future purposes; and
3. data collected to be accurate, complete, relevant, not misleading and where necessary, kept up to date. However, while updating the data, accuracy of the data and the purpose for which the data was collected need to be considered. Continuous updating is required regardless of the facts that the data may or may not be used for continuing decision or action.

Article 17 allows the data subject to access and correct the personal data. In addition, the data subject is given the right to be informed of the collection of data and the purpose of such collection at reasonable intervals without undue delay or undue expense. Facts like the nature of the personal data, the purpose of collection, and the frequency of alteration of the personal data need to be analyzed in deciding what can be considered as reasonable intervals and undue delay. The data subject is also given the right to access and correct the personal data.

Article 16 ensures that the security of personal data is protected by implementing appropriate technical and organizational measure against unauthorized or accidental access, processing or erasure, alteration, disclosure or destruction. In order to ensure security the nature of personal data held, the harm that results in such process or activities, the place where the data is held, the

security measures incorporated into any equipment, etc., need to be analyzed before the data are put in use. The data users should be duty bound to have secured and highly reliable systems to prevent others from unauthorized access, like hacking or cracking, etc.

One of the important features in this law is found in Article 35. According to this article, a data subject could file a case for compensation if his data privacy is violated. By this provision, a gap in law has been filled as the other existing laws only give way for criminal liability. Unfortunately, the law is restricted in its application. It only covers one part or district or free zone of Dubai, namely the Dubai Financial Center (DIFC). Thus the law can be applied to users who are utilizing e-Government services in DIFC only, and has no application beyond DIFC.

Besides the above-mentioned legislation, the UAE Federal Law No.2 of 2006 on cybercrimes can also be used to protect the privacy and security of the e-Government users. This law focuses on criminal actions committed using the Internet or information technology. Article 2 of the 2006 law punishes any intentional act resulting in abolishing, destroying or revealing secrets or republishing personal or official information. Article 6 criminalizes inserting information through electronic means to stop or break down or delete or alter information. Article 10 penalizes identity theft and imposes imprisonment. Article 11 prohibits abusing credit card or other electronic cards. These provisions are useful to deter anybody from accessing, misusing or altering the personal information provided by the e-Government users. In addition, Article 22 makes it a crime to log on to government websites to obtain secret information. Deleting, destroying or publishing the secret information is also punishable under the same provisions. This not only catches the actual offenders, it also catches anyone who assists or abets in committing any of the crimes mentioned under the Act. The major weakness of this legislation is that it does not provide any possible platform for providing compensations to the victims; rather it focuses on punishing the offenders. In addition, all the legislation will be ineffective if data are kept outside the UAE's jurisdiction, as the legislation has no extra-territorial effect. Thus the local government needs to take extra measures if it chooses to make use of Cloud computing facilities.

The content analysis about laws in Dubai shows that there are general laws on personal data privacy and security protection of the e-Government users. The Federal Constitution, Penal Code and the Computer Crime Act criminalize misuse of personal data. In addition to the aforesaid legislation the Dubai Electronic Transactions and Commerce Law also could be used to protect e-Government users' data privacy and security. However, the major problem with this law is that the exclusions affect three major industries, those that are the backbone of Dubai's commercial activities. The amendment to this exclusion seems necessary to provide better protection for e-Government users in all spectrums of commercial activities. The Data Protection Law is one of the best laws in Dubai and the Middle East in protecting data privacy. However, its application is limited to Dubai Financial Center only. So extending this law to the whole of Dubai or passing e-Government privacy and security laws will attract more participants to e-Government application.

## 6. Conclusion

The research analysis on privacy demonstrates that the public still places a high value on the concept of privacy and data protection, even if a deep understanding of the privacy regime may be lacking. The lack of a deeper understanding of the application of privacy and data protection may be attributed to the lack of awareness of data protection as a fundamental right. The users disapproved of the concept of data sharing between private and public sectors, and the public displays a significant fear regarding data processing. The research also shows that users consider that they may lose control over their data and that there are enforcement and application problems. (Hallinan, Friedewald & McCarthy, 2012). Like privacy, security is considered a very important factor that encourages the users of any e-Government service to shy away from full utilization. The fear of privacy and security is greater with the introduction of Cloud computing services in e-Government. Dubai is not an exception to this trend. As illustrated in the literature review, the survey conducted revealed that ensuring security and privacy, and providing ease of use of navigation are significant for the enhancement of e-Government adoption. All the constructs included in the study were found to be significant in enhancing the overall satisfaction and therefore the e-Government adoption.

The finding of this study has theoretical and practical implications. Since there have been few studies on user-centric research in the Middle East Region and there is a dearth of literature in particular about the Dubai e-Government adoption, this study fills the existing gap in this area. It provides an insight into the issues related to user adoption and concern over security and privacy. The finding reconfirms perceived security; privacy and ease of use are important factors that influence e-Government adoption. The research also establishes that even if there is no specific regulation on e-Government information security laws, the existing legislation could be extended to cover security and privacy violations. The current legal framework provides criminal sanctions against any violators. In ensuring the appropriate legal framework for privacy and security protection, the precautionary principle could benefit privacy protection since it incorporates prudence and transparency. Precaution is a general duty by which liability combined with prudence will imply that one should avoid harming others (Costa, 2012). Another measure that could be used in ensuring privacy is the introduction of privacy impact assessment (PIA). PIA could be used to evaluate systematically the potential effects on privacy of a project or initiative so that all possible stakeholders could be consulted to mitigate or avoid possible risks. This could provide a useful facility for the greater utilization of e-Government services without fear of any privacy and security violation (Clarke, 2009).

The practical contribution of the research is that it could add value to decision-makers when considering the extent of user adoption and barriers to adoption. The finding on the user adoption of e-Government services could help to evaluate the success in realizing current strategies and an action plan, and also to formulate new guidelines, strategies and objectives for the further development of e-Government. An important implication of this conclusion for administrators of e-government services is to become more customer-centric. In addition, the regulators might re-consider the adequacy of laws and regulation to allow for inter-agency electronic exchange of files and facilitate coordination between government agencies, and to guarantee the protection of privacy and the security of financial and personal data.

**REFERENCES**


Acquisti, A., Gritzalis, S., Lambrinoudakis, C., & Capitani de Vimercati, S. (2007). Digital Privacy: Theory, Technologies and Practices, Boca Raton, FL: Auerbach Publications.

Anderson, R., Brown, I., Clayton, R., Dowty, T., Korff, D., & Munro, E. (2006). Children's Databases – Safety and Privacy. Wilmslow: Information Commissioner's Office.

Bannister, F.(2005). The Panoptic State: PRIVACY, Surveillance, the Balance of risk, Information Policy. 10 (1&2), 65-78.

Barnes, S. & Vidgen. R. (2003). Interactive e-government: evaluating the web site of the UK Inland Revenue. Journal of Electronic Commerce in Organisations, 2(1), 22.

Baum, C. & Di Maio, A. (2008). Gartner‟s Four Phases of E-Government Model. Gartner Group Research, 2001, available at: http://aln.hha.dk/IFI/Hdi/2001/ITstrat/Download/Gartner_eGovernment.pdf. (Accessed 5 October 2011)

Bellamy, C., Raab, C., & Perry, T. (2005a). Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy (part 1). Public Administration, Vol. 83 No.1, pp.111-33.
Bellamy, C., Raab, C., Perry, 6. (2005b), "Joined-up government and privacy in the United Kingdom: managing tensions between data protection and social policy (part 2)", Public Administration, 83(2), 393-415

Bloom, P. N., Milne, G. R., & Adler, R. (January, 1994). Avoiding misuse of new information technologies: Legal and societal consideration. Journal of Marketing, 58, 98–110.

Burn, J. & Robins, G. (2003). Moving towards e-government: a case study of organisational change processes. Logistic Information Management, 16(1), 25-35.

Carey, P. (2009). Data Protection: A Practical Guide to UK and EU Law, 3rd ed., Oxford: Oxford University Press.

Carter, L. &.Belanger, F. (2005). The utilization of e-government services: citizen trust, innovation and acceptance factors. Information Systems Journal, 15(1), 5-25.

Caudill, E. M., & Murphy, P. E. (2000). Consumer Online Privacy: Legal and Ethical Issues. Journal of Public Policy and Marketing, 19(Spring), 7–19.

Cespedes, F.V. & Smith, J.H. (1993). Database marketing: new rules for policy and practice, Sloan Management Review, 34, 7-22.

Cheng, F.C. & Lai, W.H. (2012). The Impact of Cloud Computing Technology on Legal Infrastructure within Internet—Focusing on the Protection of Information Privacy. Procedia Engineering, International Workshop on Information and Electronics Engineering, 29, 241 – 25.

Choudrie, J., Vishanth, W. & Jones, S. (2005). Realising e-government in the UK: rural and urban challenges. Journal of Enterprise Information Management, 18(5), 568-585.

Clarke, R. (1999). Internet privacy concerns confirm the case for intervention. Communication of the ACM, 42, 60-67.

Clark, R. (2009). Privacy impact assessment: Its origins and development. Computer Law & Security Review, 25, 123–135.

Costa, L (2012). Privacy and the precautionary principle" Computer Law & Security Review, 28, 14- 24.

Cullen, R (2009). Culture, identity and information privacy in the age of digital government.Online Information Review, 33(3), 405 -421.

Culnan, M.J. (1993). How did they get my name? an exploratory investigation of consumer attitudes toward secondary information use. MIS Quarterly, 17, 341-62.

Culnan, M.J. & Milne GR, (2001), The Culnan – Milne Survey on Consumera and Online Privacy Notices:Summary of Responses. "http://www.ftc.gov/bcp/workshops/glb"

Curtin, G.C., Sommer, M.H. & Vis-Sommer, V. (2003). The world of e-government. New York: The Haworth Political Press, 1-16.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-340.

Davison, R. & Martinsons, M. (2003). Guest Editorial, Cultural Issues and IT Management: Past and Present. IEEE Transactions on Engineering Management, 50(1), 3-7.

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. Information Systems Research,17(1), 61-80.

Dunleavy, P. (2002). Better Public services through e-government. Report by Comptroller and Auditor General. London: National Audit Office Press.

European Commission. (2004). Top of the web: User satisfaction and usage survey of e-government services. E-government Unit DG Information Society, available at: http://europa.eu.int/information_society/activities/egovernment_research/doc/top_of_the_web_report_2004.pdf. (Accessed 5 October 2011). Evaristo, R. (2003). Cross-cultural research in IS. Journal of Global Information Management, 11(4) 1-3.

Foley, P., Ximena, A., & Al Sakko, M. (2006). Information sharing for social inclusion in England: a review of activities, barriers and future directions. Journal of Information, Communication and Ethics in Society, 4(4), 191-203.

Fox, S. & Beier, J. (2006). Online banking 2006: surfing to the bank, Pew Internet & American Life Project, available at: http://www.pewinternet.org/Reports/2006/Online- www.pewinternet.org/Reports/2006/Online- Accessed 5 October 2011)

Gilbert, D. & Balestrini, P. (2004). Barriers and Benefits in the adoption of e-government. The International Journal of Public Sector Management, 17(4) 286-301.

Hallinan, D., Friedewald, M. & McCarthy, P. (2012). Citizens' perceptions of data protection and privacy in Europe. Computer Law & Security Review,28, 263 -272.

Hiller, J.S. & Cohen, R. (2001). Internet Law and Policy. Upper Saddle River, NJ:Prentice-Hall,.

Hoffman, D.; Novak, T. & Peralta, M. (1999). Information privacy in the marketspace: implications for the commercial uses of anonymity on the Web. The Information Society, 15(2), 129-139.

Horan, T.A. & Abhichandani, T. (2006). Evaluation user satisfaction in an e-government initiative: Results of structural equation modeling and focus group discussions. Journal of Information Technology Management, 17(4), 33-44.

Howard, M. (2001). E-Government Across the Globe: How Will E- Change Government? Government Finance Review, 17(4) 6-9.

Khan S. (2010). Apps.Gov: assessing privacy in the cloud computing. NCJL & Tech, 11, 259-289.

Kim, D.J., Song, Y.I., Braynov, S.B., & Rao, H.R. (2005). A multidimenstional trust formation model in B-to-C e-commerce: a conceptual framework and content analyses of academia/practitioner perspectives. Decision Support Systems, 40, 143-165.

Koufaris, M. & W. Hampton-Sosa (2004). The Development of Initial Trust in an Online Company by New Customers. Information & Management, 41(3), 377-397.

Laczniak, E.R. & Murphy, P.E. (1993). Ethical Marketing Decisions: The Higher Road. Boston, MA: Allyn and Bacon.

Lam, W. (2005). Barriers to e-government integration. Journal of Enterprise Information Management, 18(5), 511-530.

Layne, K. & Lee, J. (2001). Developing fully functional e-government: A four stage model. Government Information Quarterly, 18(2), 122-136.

Lee, S.M., Tan, X. & Trimi, S. (2005). Current practices of leading e-government countries. Communication of the ACM, 48(10), 99-104.

Lee, J. (2010).10 year retrospect on stage models of e-Government: A qualitative meta-synthesis. Government Information Quarterly, 27, 220–230

Liu, C, & Chen, K (2011). Examining the impact of privacy, trust and risk perceptions beyond monitory transactions: An Integrated model. Electronic Commerce Research and Applications, 10, 702–715,

Mintzberg, H. & Westley, F. (1992). Cycles of Organizational Change. Strategic Management Journal, 13, 39-59.

Miyazaki, A.D. & Fernandez, A. (2001). Consumer perceptions of privacy and security risks for online shopping. The Journal of Consumer Affairs, 35(1), 27-44.

Mohamed, N. & Ahmad, I.H. (2012). Information privacy concerns, antecedents and privacy measure use in social networking sites: Evidence from Malaysia. Computers in Human Behavior, 28, 2366–2375

Murphy, J. (2005). Beyond E-Government the world's most successful technology-enabled transformations, Booz Allen Hamilton: The INSEAD Business School for the World,1-124.

Nam, C., Song, C., Lee, E., & Park, C. (2006). Consumers Privacy Concerns and Willingness to Provide Marketing-Related Personal Information Online. Advances in Consumer Research, 33, 212-217.

Norris, D.F., & Moon, M.J. (2005). Advancing e-government at the grassroots: Tortoise or hare? Public Administration Review, 65(1), 64-75.

OECD (2004). Information and Communication Technologies: OECD Technologies Outlook: 1-278", available at: http://www.oecd.org/dataoecd/22/18/37620123.pdf (Accessed 8 October 2011). On the Acceptance of Electronic Commerce", International Journal of Electronic Commerce, 73, 135-161.

Pavlou, P.A. (2003). Consumer acceptance of electronic commerce: integrating trust and risk with the technology acceptance model. International Journal of Electronic Commerce, 7(3), 101-134.

Phelps, J., Nowak, G. & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. Journal of Public Policy & Marketing, 19, 27-41.

Pincus, L.B., & Johns, R. (1997). Private parts: a global analysis of privacy protection schemes and a proposed innovation for their comparative evaluation. Journal of Business Ethics, 16, 1237-1260.

Pitt, L.F., R.T. Watson, & Kavan, C.B. (1995). Service quality: A measure of information systems effectiveness. MIS Quarterly, 19(2), 173-188.

Raja, V.T., & King, N.J. (2012). Protecting the privacy and security of sensitive customer data in the cloud. Computer Law and Security Review, 28, 308 – 319.

Reddick, C.G. (2004). The Growth of E-Procurement in the U.S. States: A Model and Empirical Evidence. Journal of Public Procurement, 4(2), 151-176.

Reidenberg, J.R. (1996).Governing networks and rule-making in cyberspace. Emory Law Journal, 45, 896-97 Safire, W. (2002). The intrusion explosion. The New York Times, (May 2), 27.

Sarikas, O.D., & Weerakkody, V. (2007). Realising integrated e-government services: A UK local government perspective.Transforming Government: People, Process and Policy, 1(2), 153-173. Schneier, B.(2010). ―Privacy and Control,‖ Schneier on Security, April 26, availableathttp://www.schneier.com/blog/archives/2010/04/privacy

Schneier, LR, August 20, 2007, "your data are less safe today than 2 years ago", Computer World, available at http://www.computer world.com

Sheehan, K.B. and Hoy, M.G. (1999), "Flaming, complaining, abstaining: how online users respond to privacy concerns", Journal of Advertising, Vol. 28, pp. 37-51.

Singh, A., Liu, L., Ahamad, M. (2008), "Privacy analysis and enhancements for data sharing in *nix systems", International Journal of Information and Computer Security, Vol. 2 No.4, pp.376-410.

Smith, H. J., Milberg, S. J., & Burke, S. J. (1996). Information privacy: Measuring individuals' concerns about organizational practices. MIS Quarterly, 20 (June), 167–196.

Solove, D. J. 2008. Understanding Privacy. Cambridge, Massachusetts: Harvard University Press.

Sotto L.J., Treacy B.C., and McLellan M.L. (2010) "Privacy and data security risks in cloud computing", Electronic Commerce & Law Report, Vol. 15, p.186

Strader, T. J., Shaw, M. J. (1997): Characteristics of electronic markets. Decision Support Systems, 21, 185-198.

Suh, B. & Han, I.(2003). The Impact of Customer Trust and Perception of Security Control on the Acceptance of Electronic Commerce. International Journal of Electronic Commerce, 73, 135-161.

Van de Donk, W. (Eds), Visions of Privacy: Policy Approaches for the Digital Age, Toronto: Toronto University Press, 113-33.

Van Slyke, C., Shim, J. T., Johnson, R., & Jiang, J. (2006). Concern for Information Privacy and Online Consumer Purchasing. Journal of the Association for Information Systems 7(6), 415-443.

Warkentin, M., Gefen, D., Pavlou, P.A., & Rose, G.M. (2002). Encouraging citizen adoption of e-government by building trust, Electronic Markets, 12(3), 157-162.

Warren, A. (2002). Right to privacy? The protection of personal data in UK public organisations. New Library World, 113(11/1)2, 446-56.

Weerakkody, V., & Dhillon, G. (2008). Moving from e-government to t-government: A study of process reengineering challenges in a UK local authority context. International Journal of Electronic Government Research, 4(4), 1-16. Westin, A.F. (1967), Privacy freedom: New York: Athenem.

Wolfinbarger, M., & Gilly, M.C. (2003). eTAILQ: dimensionalizing, measuring, and predicting etail quality. Journal of Retailing, 79(3), 183-198.

Wolfinbarger, M & Gilly, M. (2001). Shopping online for freedom, control, and fun. California Management Review, 7(3), 7-37

Wu, K.W., Huan, S.Y., Yen, D.C. & Popova, I. (2012). The effect of online privacy policy on consumer privacy concern and trust. Computers in Human Behavior, 28, 889–897.

Zhao, J.J., & Zhao, S.J. (2010). Opportunities and threats: A security assessment of state e-government websites. Government Information Quarterly, 27, 49–56.